REMARKS

The above Amendments and these Remarks are in reply to the Office Action mailed December 14, 2004. Currently, claims 1-43 are pending. Claims 1, 19, and 36 have been clarified. Claims 1-43 are presented herewith for consideration.

Rejection of Claims 1-7, 11, 12, 14, 16, 19-24, 28, 29, 31, 33, 36-40 Under 35 U.S.C. § 102(b)

Claims 1-7, 11, 12, 14, 16, 19-24, 28, 29, 31, 33, 36-40 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,923,756 to Shambroom ("Shambroom"). Applicants respectfully traverse the rejection with respect to these claims as follows.

Shambroom relates to a method for providing secure remote command execution over an insecure network. Specifically, Shambroom discloses the use of a key distribution server (KDC). Shambroom specifically discloses the use of Kerberos, a type of key distribution system for providing secure remote command execution over an insecure computer network. The key distribution server acts separately from a primary server to provide secure access between a client and a primary server. Shambroom states in this regard:

> One example of a secret-key based network authentication system is the trusted third-party authentication service called Kerberos. Network services and clients requiring authentication register with Kerberos and receive a secret key, where said key (or a pass phrase from which it can be derived) is known only to the user and a Kerberos host server. Kerberos also generates temporary session keys, which can be used to encrypt messages between two registered Kerberos principals (users or hosts). A typical Kerberos software package is Kerberos Version 5 from Project Athena at the Massachusetts Institute of Technology (MIT). The Kerberos authentication scheme also is discussed in J. Kohl and C. Neuman, The Network Authentication Service (V5), Request for Comments: 1510 (September 1993). Kerberos and other trusted third-party private authentication schemes can allow for speedier, secure access between two principals. (Shambroom Col. 2, Lines 35-51).

Each of the claims 1-43 recites in part

(a) creating a log-in record, wherein said log-in record includes an encrypted version of a primary system client identifier;

(b) said intermediate system receiving log-in data for said client;

(c) authenticating access of said client to said intermediate system, based on data from said log-in data and data from said log-in record;

(d) sending authentication data to said primary system, wherein said authentication data includes data from said primary system client identifier; and

(e) performing authentication on the primary system using the data from the said primary system client identifier.

At least the features of (d) sending authentication data to said primary system, wherein said authentication data includes data from said primary system client identifier, and (e) performing authentication on the primary system using the data from the said primary system client identifier, are nowhere disclosed, taught or suggested by Shambroom.

Shambroom teaches that a secure connection between the key server and the client is created based on the username and password. The key server then generates a session and keys. These keys are different from the username and the password that the client used to gain access to the key distribution server so that they will not expose the client's username and password to an insecure network where hackers might acquire it. Shambroom States:

> Once web server 305 receives encrypted login information from web browser 205 as indicated by arrow 356, network server 300 passes the Kerberos user principal name of client 200 and a request for a permission indicator to KDC 400 over insecure network 350 as indicated by arrow 352. Upon receiving the request for a permission indicator at 352, the KDC 400 generates a KDC session key for protecting transactions between network server 300 and KDC 400. (Shambroom, Col 8, 19-26).

The examiner has argued that Shambroom discloses the element of sending authentication data to said primary system, wherein said authentication data includes data from said primary system client identifier. In support of this argument the examiner has cited the following language from Shambroom:

> Network server 300 then encrypts the message or command, using the server session key and, as indicated at arrow 364, sends the encrypted message along with the access indicator and a new authenticator to destination server 500 via insecure network 450. Destination server 500 uses its own private key to decrypt and obtain the server session key. (Shambroom Col. 9 Lines 39-45).

The applicants respectfully assert that the quoted language relates to transmission of session keys, which are credentials as taught by Shambroom. As will be explained in depth

hereinafter, the credentials taught by Shambroom do not anticipate the presently claimed invention.

Shambroom teaches that the keys are not username and password data for use on a primary systems. Shambroom teaches that the username and password should be transmitted to the intermediate server which, after authentication on the intermediate server, will generate credentials, which are different from the username and password. Shambroom discloses the use of sessions and keys:

> Using client 200's Kerberos user principal name received at 352, the KDC 400 extracts client 200's secret key from key database 405, which stores secret keys used by KDC 400 and other properly registered clients. Using client 200's secret key, the KDC 400 then encrypts one copy of the KDC session key and creates a permission indicator, which would typically include by way of example only, a timestamp, client 200's user name and network address, and another copy of the KDC session key. This permission indicator will be used later by client 200 to authenticate itself to KDC 400. The permission indicator is encrypted with KDC 400's private key, which is known only to KDC 400; KDC 400, therefore, can later decrypt the permission indicator to verify its authenticity. (Col 8, 27-41).

Shambroom teaches that once the keys are generated the client and server use them to communicate with each other securely. Shambroom teaches that sessions and keys should be used to avoid transmitting a username and password. Shambroom teaches that the motivation for doing so is that if compromised by a hacker the username and password will not be compromised. Shambroom states:

> KDC 400 then sends both the encrypted session key and the permission indicator back to the network server 300 as indicated at arrow 354. Network server 300 receives the encrypted information from KDC 400, and decrypts the KDC session key using client 200's user key. In one embodiment, the client user key is a one-way hash of client 200's password and other information, so the network server is able to derive the user key by hashing client 200's password. Both the permission indicator and the KDC session key are stored in credentials cache 320. Web server 305 encodes the contents of the credentials cache 320 and, as indicated at arrow 357, sends the contents of the credentials cache 320 to web browser 205. The authenticating information that may have resided in the network server 300 is then erased or otherwise deleted. Thereafter, in order for client 200 to continue with the transaction, client 200 will have to refresh the memory of server 300. If a hacker or interloper managed to gain access to network server 300 while information was stored in credentials cache 320, only the permission indicator and session key could be obtained, because the Kerberos password is destroyed after being used. This information would be of limited value, however, because the permission indicator, in the preferred embodiment, would contain a date/time stamp and would

become worthless after a specified period of time, usually relatively short, has elapsed. (Col 8, 41-67).

The examiner in making his rejection listed the element as "sending authentication data to the primary system." This omits the limitation "wherein said authentication data includes data from said primary system client identifier." According to MPEP § 2131 a rejection may be overturned for a failure to teach every element of the claim.

Thus the applicants assert that at least the elements of (d) sending authentication data to said primary system, wherein said authentication data includes data from said primary system client identifier; and (e) performing authentication on the primary system using the data from the said primary system client identifier, are not taught or suggested by Shambroom.

Based on the above it is respectfully submitted that Claims 1-7, 11, 12, 14, 16, 19-24, 28, 29, 31, 33, 36-40 are not disclosed in Shambroom, and it is respectfully requested that the rejection of these claims on section 102 grounds be withdrawn.

Rejection of Claims 13, 15, 30, and 32 under 35 U.S.C. § 103(a)

Claims 3-6, 9, 12, 15, 28, 34-37, 40, 56-58, and 60 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Shambroom in view of U.S. Patent No. 5,418,854 to Kaufman et. al ("Kaufman").

Applicants respectfully traverse the rejection as follows:

Kaufman teaches a login agent for a client. The login agent is semi trusted meaning that it is not trusted with the user's password, however, it is trusted with the ability to grant the user a key to the primary system. The variables Kaufman uses are as follows: D is a credential, M is a message from the client to the Login Agent (normally encrypted containing the username and password). N is the username, H2 and H1 are hash totals generated for the Login Agent, and workstation 12 is the workstation seeking a key or credential. Kaufman discloses:

> Upon reception of M, the LA 26 parses the username N, decrypts the encrypted portion of the message M using its private key and temporarily stores $H2_A$ and K in a local buffer 32. The LA's private key is also stored in the buffer 32. The LA

then forwards (at reference 42) the username N to the CSS 24, which searches for the name in its directory service 25. Upon locating N, the CSS 24 obtains the associated doubly-encrypted credential D and forwards it (at reference 44) to the LA 26. As noted, D contains the user's private RSA key U encrypted with H1, $\{U\}_{H1}$; this quantity is appended to H2 and further encrypted under the LA's public key, $\{\{U\}_{H1,H2}\}_{LA\text{-}PUB}$, to prevent comprehension by arbitrary users. (Kaufman, Col 7, 65 - Col 8, 11).

Each of Claims 13, 15, 30, and 32 recite in part

(a) creating a log-in record, wherein said log-in record includes an encrypted version of a primary system client identifier;

(b) said intermediate system receiving log-in data for said client;

(c) authenticating access of said client to said intermediate system, based on data from said log-in data and data from said log-in record;

(d) sending authentication data to said primary system, wherein said authentication data includes data from said primary system client identifier; and

(e) performing authentication on the primary system using the data from the said primary system client identifier.

Applicants respectfully submit that as discussed above, at least the features of (d) sending authentication data to said primary system, wherein said authentication data includes data from said primary system client identifier, and (e) performing authentication on the primary system using the data from the said primary system client identifier, are nowhere disclosed, taught or suggested in Shambroom. Kaufman adds nothing to the teachings of Shambroom in this regard.

The examiner argues that Kaufman teaches the element of verifying the client identifier and the client password. Applicants assert that Kaufman does not teach this step. In support of the rejection the examiner cited the following language:

> The workstation decrypts E with the secret nonce key K stored in the buffer 13 and then decrypts the resulting encrypted credential with $H1_A$ to obtain the user's private key $U.H1_A$ is equal to H1 because it has already been established that the entered password was correct. With possession of its key U, the workstation can now participate in public key-based authentication protocols on behalf of the user. correspond to the client. (Kaufman Col. 8, Lines 26-33)

A careful reading of Kaufman results in the finding that once the Login Agent has determined that the workstation seeking access has a proper username and password, it sends the workstation a credential which the workstation can use to communicate with the server. According to Kaufman, this credential is encrypted. It is referred to as E, where E is defined as "E = $\{\{U\}_{H1}\}_K$." The login agent passes this to the workstation if the workstation is authenticated. Here Kaufman discloses $H1_A$ and $U.H1_A$ (which the examiner has argued are the client username and password for the purposes of verification):

> Referring to FIG. 5, the LA 26 decrypts D with its own private key to obtain the encrypted credential $\{U\}_{H1}$ and to obtain H2. The LA then compares $H2_A$ received from the workstation to H2 extracted from D. If the hash totals do not match, the LA 26 does not return any further information and may audit the unauthorized user's login attempt, depending on local policy. In any event, the LA 26 terminates the login procedure. If a match ensues, it is apparent that the workstation 12 is in valid possession of the user's password; therefore, the LA 26 encrypts the encrypted credential with K to form a modified encrypted credential E, i.e., $E=\{\{U\}_{H1}\}_K$, and then forwards E (at reference 50) to the workstation 12. (Kaufman, Col 8, 11-25)

When read in light of the entire disclosure of Kaufman, it is clear that $H1_A$ and $U.H1_A$ are hash totals calculated in the creation of sessions and keys as disclosed by Kaufman in Col. 7 lines 51-52 under the heading Logging-In. Thus the Kaufman does not disclose teach or suggest the applicants' claimed invention.

Based on the above it is respectfully submitted that Claims 13, 15, 30, and 32 under 35 U.S.C. § 103 are not disclosed taught or suggested by Shambroom. Kaufman adds nothing to the teachings of Shambroom in this regard. Each of claims 13, 15, 30, and 32 depend directly or indirectly on claims 1 or 19 incorporating the limitations of its respective base claim therein. As discussed above, Shambroom does not teach or suggest the elements of claims 1 and 19. Thus, it is respectfully submitted that the invention recited in claims 13, 15, 30, and 32 under 35 is not taught or suggested in the cited references, taken alone or in combination with each other.

Based on the above amendments and these remarks, reconsideration of claims 1-43 is respectfully requested.

The Examiner's prompt attention to this matter is greatly appreciated. Should further questions remain, the Examiner is invited to contact the undersigned agent by telephone.

Enclosed is a PETITION FOR EXTENSION OF TIME UNDER 37 C.F.R. § 1.136 for extending the time to respond up to and including today, June 14, 2005.

The Commissioner is authorized to charge any underpayment or credit any overpayment to Deposit Account No. 501826 for any matter in connection with this response, including any fee for extension of time, which may be required.

Respectfully submitted,

Date: 6/14/05

By: _____

Walter K. Coronel
Reg. No. 56,177

VIERRA MAGEN MARCUS HARMON & DENIRO LLP
685 Market Street, Suite 540
San Francisco, California 94105-4206
Telephone: (415) 369-9660
Facsimile: (415) 369-9665